Indo-Iranian Journal of Scientific Research (IIJSR)
(Quarterly International Journal) Volume 3, Issue 1, Pages 69-84, January-March 2019

# Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes

Dr. Vinod Varma Vegesna

*Sr. IT Security Risk Analyst, The Auto Club Group, United States of America. Email: vinodvarmava@gmail.com*

Article Received: 30 August 2018 Article Accepted: 29 November 2018 Article Published: 26 January 2019

ABSTRACT

Cloud computing is a computer platform that enables users to pool information such as infrastructure, programs, services, and workflows. The cloud is a virtual pool of computational resources. It makes available computer resources in a group to consumers via the network. Cloud computing, as a new computer architecture, intends to openly share a memory, processing, and applications across a large number of clients. Current cloud computing systems have significant limitations in terms of ensuring clients' information confidentially. Because clients' sensitive information is transported in plaintext form to distant workstations controlled and maintained by third-party telecommunications companies, the danger of unauthorized exposure of clients' confidential documents by telecommunications companies is rather significant. A number of methods exist for securing clients' information against external intruders. This paper elaborates on the most recent situation in the investigations of various security protocols for data protection in cloud-based infrastructures.

**Keywords:** Cloud computing, Storage, Data protection, Enhanced security, Software models.

## 1. INTRODUCTION

The cloud is an Internet-based computer system that provides clients with on-demand access to common services such as applications, systems, memory, and data. Cloud computing platforms offer a variety of web information storage and customer support. Cloud computing, together with the rapid expansion of the Internet, is receiving huge traction in recent times as a new approach of pervasive computing for a variety of applications, particularly for enterprise systems, due to its numerous main advantages, such as economic feasibility and high flexibility and scaling [1-4]. Issues regarding Internet security are growing as the Cloud services era advances, regarding how can cloud customers understand whether their data would be accessible, safe, and protected against intrusion [5].

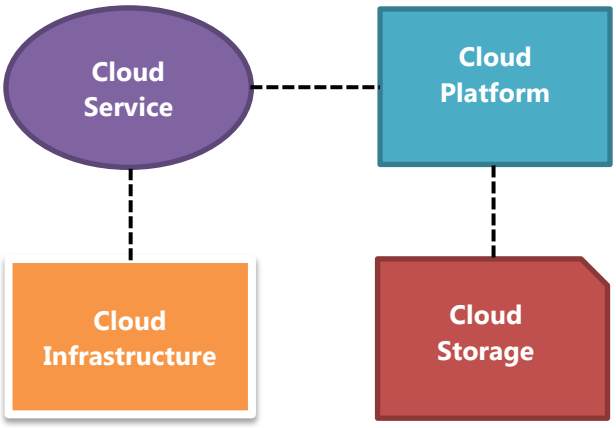


**Figure 1.** Cloud Computing Operational Infrastructure

In cloud computing, the expression Cloud refers to a telecommunications network or a system that is integrated with computational equipment. Whenever a client requests applications, devices, or processing capabilities, the cloud computing system is accessible over the internet. Cloud computing is a virtual pool containing system resources that is accessible to consumers over the internet. Figure 1 depicts a typical infrastructure for cloud computing.

Cloud computing delivers a wide range of features to users by assembling groups and networks of systems. The major purpose is to deliver solutions in a virtual fashion to lessen the strain on the consumer to manage anything on their own. It might also apply to internet technology that offers computers with a common resource pool that includes data, or applications on a cost basis. Rather than getting individual infrastructure or personal devices to handle programs, individuals adopt the Cloud computing paradigm of pooling computer resources.

Cloud computing offers a platform wherein users may establish their own virtualized resources and conduct operations without regard for geographical limitations. Individuals are drawn to Cloud services that are already connected to Platforms, applications, or infrastructures due to the diverse environment and lower cost [6-10]. There are three implementation options for cloud computing depending on their use: public cloud, private cloud, and hybrid cloud. The cloud-based deployment strategies are shown in Figure 2.

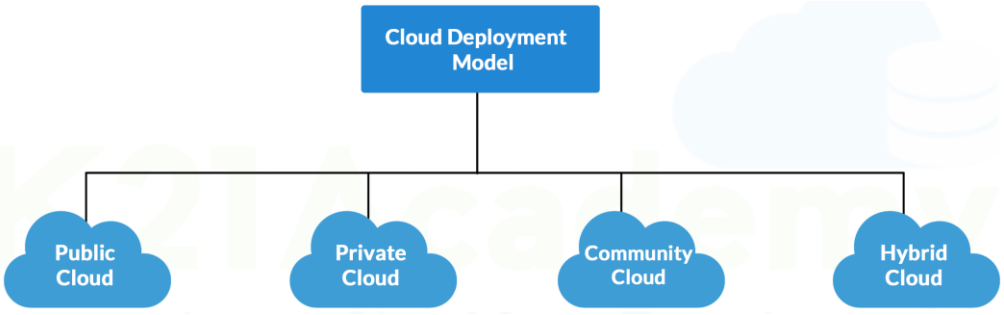


**Figure 2.** Cloud-based deployment strategies

Cloud computing offers various better services to customers, but it also has a number of drawbacks such as authenticity or memory accuracy, reliability, privacy, and others. These issues arising from clients' adaptation to the cloud infrastructure are relatively challenging. As a result, much study is necessary throughout this area to establish cloud users' confidence in cloud providers.

### *1.1. Cloud Computing Services*

As seen in Figure 3, the cloud delivers 4 kinds of services depending on the various needs of customers. Cloud service companies offer a variety of software as a service. It results in more efficient memory consumption on computers. In the growing market, SaaS vendors supply the greatest computing systems such as applications, networking space, and data centers. Salesforce.com and Google Apps are illustrations of SaaS. Cloud computing entails a network of systems that work together to perform various calculations and activities. Cloud computing has emerged as among the most prominent IT trends of recent times.

Among the primary advantages of using IT technologies for businesses is decreased market time and expenses. Cloud computing allows businesses and organizations to access pooled processing and storage resources. It is preferable to construct and run their individual infrastructures. Cloud computing likewise offers organizations and businesses an IT platform that is scalable, safe, and cost-effective. It is comparable to global electric grids, which let enterprises and families connect to a highly regulated, reliable, and premium energy supply. Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle, and Novell are among the major organizations that have ventured into cloud computing and provide a variety of internet products to people and enterprises.

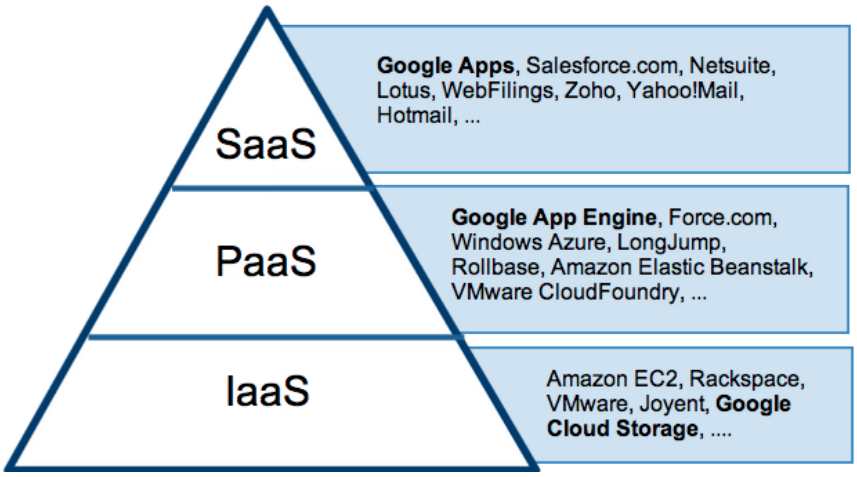


**Figure 3.** Models of cloud services

In terms of the numerous benefits delivered, a variety of categories and paradigms exist in cloud computing. As a result, cloud computing encompasses public clouds, private clouds, hybrid clouds, and community clouds. Service delivery methods, on the contrary side, may be classified as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Cloud computing is often characterized in two aspects: by cloud computing locations and by the variety of services supplied. Cloud computing is usually categorized by cloud position as follows: public cloud (in which the data center is offered to host by the cloud provider); private cloud (in which the cloud provider is allocated to a particular organization but not distributed with other organizations); hybrid cloud (the combination of private and public clouds together); and community cloud (it involves sharing of IT infrastructure in between organizations of the same community).

Cloud computing, a unique method for digitally analyzing and transporting information, is currently employed in practically all computing devices. It operates on a network technology that is vulnerable to several forms of assault. DDoS (Distributed Denial of Service) is among the most well-known types of cyberattacks [11-17]. Syn cookies, in addition to limiting the number of clients who may access the service through cloud technologies, might be utilized to prevent Distributed Denial of Service.

Another man-in-the-middle attack can be another form of cloud-based computing assault. A secure Socket Layer (SSL) is a security feature used to counteract such abuse. As a result, if this level of security is not correctly set, verification of the clients and servers may not adequately safeguard cloud-based clients from man-in-the-middle attacks.

As a result, the safety concerns of information security while employing cloud-based applications should be addressed and reduced. In the case of cloud computing, users execute their program on hard discs and CPUs which are not physically present. As a result, people are increasingly concerned about their safety concerns when employing this system. As a result, a wide range of cyberattacks might occur with cloud infrastructure. Aside from the aforementioned, the majority of common threats include phishing, IP spoofing, document manipulation, packet analysis, IP gateways, and so on. A number of information security privacy approaches approved by cloud computing companies, all of which include authentication, secrecy, password protection, and authorization.

## 2. CLOUD COMPUTING CONFIDENTIALITY

One of the most important critical security measures for cloud customers' information security is confidentiality. It encrypts the unencrypted cipher text prior to actually storing the information in the cloud. This technology safeguards customers' information, and sometimes even cloud service companies are unable to change or access material saved in this manner in the cloud.

Dell data security and cryptography provide such a level of safety for customers' information whenever it is saved on an external drive or media. Cryptography might be accomplished with either equipment or software [18-19]. The main advantage of using this type of security would be that customers do not have to worry about enforcing data security and privacy standards. Dell also employs Transparent File Encryption to keep track of who is viewing the information.

Wuala cloud is another company that provides security for cloud services. Whenever desktop computers communicate information to the cloud, cryptography is activated. This is exceptional security since even the supplier is unable to view the information. A few authors have observed multilayer attribute-based cryptographic techniques for cloud technology. The above-suggested security approach for cloud computing secrecy provides fast speed and excellent security systems. Several researchers offered a cryptography mechanism that allows users to govern the information they have in the cloud.

Confidentiality is also supplied by the vendor Online Tech, who achieves confidentiality in cloud applications using cryptographic techniques (such as Full Disk Encryption) which protect recorded information on storage devices during the startup process. Encrypting data using the well-established AES (Advanced Encryption Standard) technique is indeed employed with Whole Disk Encryption. If a computer that uses cloud-based computing is lost or damaged, a bit locker key is used to safeguard the information stored on the stolen or misplaced devices.

As a result, one may infer in this part as privacy is critical for securing information stored in the cloud, and different providers provide various security approaches to ensure secrecy. DELL, for instance, provides both hardware-based and software-based encryption, in addition to transparent file encryption. The advantages of this cryptography are that they are simple to install and do not necessitate user participation. Wuala employs cryptographic techniques on computers, and this form of cloud protection benefits customers in terms of information accessibility.

### *2.1. Recommendations for Improving Cloud Data Security*

Many researchers discussed the significant guidelines for maintaining a safe cloud infrastructure. One of these suggestions is for a cloud provider to guarantee the existence of better management, security, and regulatory systems [20-27].

The above implies that cloud technology should have security protocols comparable to those found in conventional IT platforms. In every case, cloud technology could also provide distinct threats to a company with conventional IT systems. As a result, whenever a business employs cloud services, customers must understand the amount of risk tolerance.

Another suggestion would be that cloud users ensure that their provider has capabilities and policies in place to govern who has access to their services and information. This one is required to ensure that accessibility to the cloud infrastructure is monitored and restricted. As a result, managing individuals, responsibilities, and credentials is critical for cloud implementation.

Whenever customer service is transferred to the cloud, the operator must enable the client to allocate their usernames and passwords to accessible categories and responsibilities that mirror their operations and business safety requirements. A useful piece of advice for cloud services security is to ensure that cloud services and communications are secured.

Internal network assaults such as breaches of privacy or the leak of private information, authenticity violations such as illegal data alteration, and resource breaches such as denial of service should be avoided by cloud users. As a result, cloud users must analyze the cloud platform company's corporate network restrictions in terms of their needs and any regulatory issues that may exist.

Another one of the primary suggestions is to evaluate infrastructure and facility security procedures. Since the facilities and infrastructure used in cloud technology are often managed and controlled mostly by the cloud provider, the cloud user is responsible for obtaining confirmation from the vendor that sufficient security precautions have been taken.

***1. Data Security in the Cloud***

The simplest method for safeguarding the cloud's information is to use a combination of cryptography, backup and recovery measures, security standards, authenticating, and authorizing procedures. Whenever manufacturers and companies utilize encryption algorithms, such methods must be widely recognized and have been recognized through NIST.

***2. Appropriate Application of Administrative Rights and protections***

The organization that uses cloud services must limit administrator rights and only use administrator credentials whenever necessary. All administrator credentials must be inventoried using automated technologies, and each user with appropriate rights on smartphones, computers, and networks must be validated by one senior executive. All administrator credentials must be complicated, containing a blend of numbers, symbols, or special characters, and no vocabulary terms. When installing some new devices in network infrastructures, all credentials for hardware and software, programs, gateways, router, access points, as well as other structures must be updated. Service accounts must also include lengthy, complicated credentials that are kept up-to-date regularly. Credentials must be encoded or hashed before being stored. Cryptographic credentials must adhere to the recommendations in NIST SP 800-132 or related documents.

***3. Data Access Control through Wireless***

Organizations that use cloud technology and have mobile channel(s) must use professional wireless scanning, surveillance, and identification technologies, as well as digital cellular intrusion detection technologies. The company's intelligence officer must collect network signals from the station's boundaries on a routine basis and use professional and open analytic software to see if the wireless communication was carried by using cryptography

that such organization approves or perhaps some inferior standards. Within that scenario, system administrators must also employ remote monitoring tools on the wired connection to obtain information about the wireless capability and devices linked to controlled space.

***4. Cloud Computing Data Recovery***

This is critical that any system that incorporates cloud technology seems to have an automated backup system in place that is updated every week, as well as for systems containing private information much more regularly. The whole backup strategy must encompass the computer's software, development tools, and information. Numerous backups over time may also be established, and recovery plans must be following any legal or legislative compliance.

***5. Data in the Cloud Boundary Defense***

Boundary protection in a cloud-based company might be achieved by utilizing public or paid IDS and detection systems to identify assaults from external factors on the company's inner technologies or vice-versa. It is also advantageous to block connections using known malicious IP addresses or to deny entry to just trustworthy sites. Companies must use infrastructure IPS systems in addition to IDS to prevent known malware identities or malicious activity. While utilizing remote login like a VPN, two-factor authentication must be used. Only DMZ servers should connect with the company's private communication networks through software proxies or software firewalls across permitted connections.

## 3. CLOUD SERVICES RISKS AND SECURITY CONCERNS

Cloud technology as well as its information are related to a number of dangers and potential vulnerabilities. Nevertheless, this study will investigate virtualization, cloud infrastructure memory, and multi-tenancy as they pertain to information security in cloud computing [28-30]. Table 1 depicts the risks and remedies associated with using the cloud.

**Table 1.** Risks and solutions related to cloud computing

| Security Risks | Attack Definition | Impacts | Solutions |
|---|---|---|---|
| **XML Signature Wrapping Attacks** | Insert new body to the original messages | Change of original data | Utilize source coding |
| **Browser Security** | Data is stored passively so the browser will not generate authentication tokens | Data losses | Utilize XML signatures |
| **Lock-in** | Complexity issue while moving from one platform provider to another | Vendor locks-in clients | Middleware, Software adoptions, Model-driven architectures |

### *A. Virtualization*

Virtualization is a technology that captures a properly operational operating system in some other OS in order to utilize all of the capabilities of the actual operating system. To execute a guest OS as a virtual environment in a host system, a specific feature known as virtualization is needed. Virtualization is a fundamental component of cloud technology that aids mostly in the delivery of cloud computing's essential ideals. Nevertheless, with cloud services, virtualization presents certain threats to information. A potential danger is that virtualization may be compromised. If a hypervisor is weak, it could be a major target. If a hypervisor is hacked, the entire computer is at risk.

The additional danger connected with virtualization is resource allocation and re-allocation. If VM operation information is written to storage and not deleted prior to reallocating storage to the subsequent VM, information disclosure to the subsequent VM may occur, that could be undesired. An improved strategy for the usage of virtualization is a remedy to the aforementioned concerns. Services must be handled with caution, and information must be adequately authorized prior to re-allocating them.

### *B. Public Cloud Storage*

A further security problem in cloud technology is information processing in a cloud platform. Clouds often use centralized storage infrastructure that might make them a tempting security risk. Memory capacities are complex systems comprised of technology and software components that might expose information if a minor violation occurs in the cloud infrastructure. To eliminate these concerns, it is usually suggested that particularly sensitive data be stored in cloud infrastructure, if feasible.

### *C. Multitenancy*

Among the greatest hazards to information in cloud technology is distributed accessibility or multitenancy. Because several customers are utilizing the same shared pool of configurable computing resources such as CPU, memory, and bandwidth, it poses a hazard to not just one but different users. There is always a possibility of private information being mistakenly leaked to certain other users in this kind of instance. Multitenancy attacks are particularly dangerous since a single error in the system might enable other hackers or users to access all other data. Such sorts of concerns may be avoided by intelligently verifying people prior to granting them access to the information. To minimize multitenancy difficulties in cloud technology, many authentications are utilized.

## 4. CLOUD COMPUTING SECURITY APPROACHES

### *1. Security of Cloud Implementation Models*

Essentially, cloud implementation is handled in-house (Private Cloud) or via a third-party site (Public Cloud). Although it has been implemented like a connected private-public cloud for a variety of purposes (Hybrid Cloud). A "Community Cloud" is a 4th kind of cloud deployment paradigm in which the architecture is distributed across multiple organizations and is accessible to a particular community [31-33]. In a private cloud setup, an organization can maintain ownership of its infrastructure or contract it to a 3rd party, whether on-site or off-site. Securing the in-house technology platform is manageable and does not necessitate the deployment of additional protection devices.

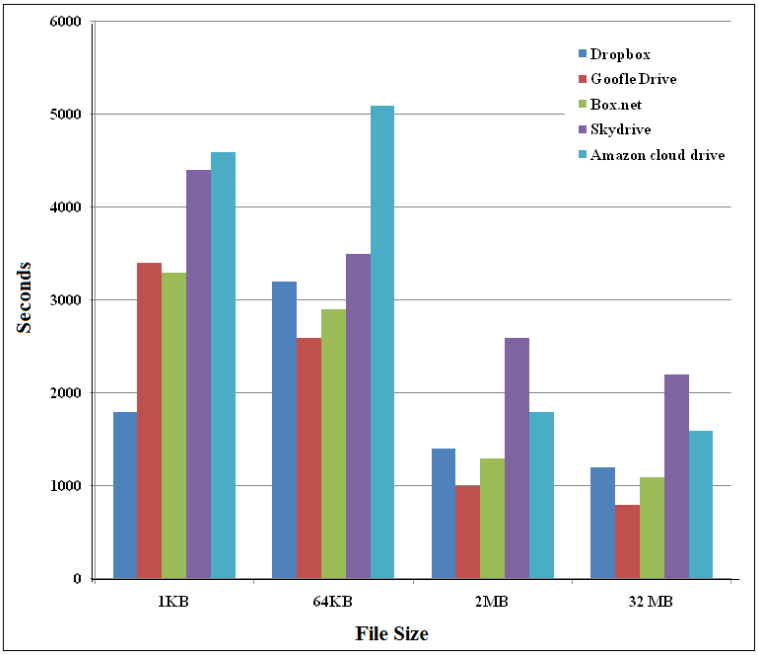


**Figure 4.** Performance of cloud storage firms

A public cloud implementation is a paradigm within which a third-party network operator delivers essential facilities on a pay-per-use basis. This strategy has many advantages, including cost savings, the opportunity to have relatively brief use, and more capabilities. Using the shared public cloud securely is more difficult than using private clouds. The public cloud is better suited for miscellaneous expenses or less susceptible programs in this case.

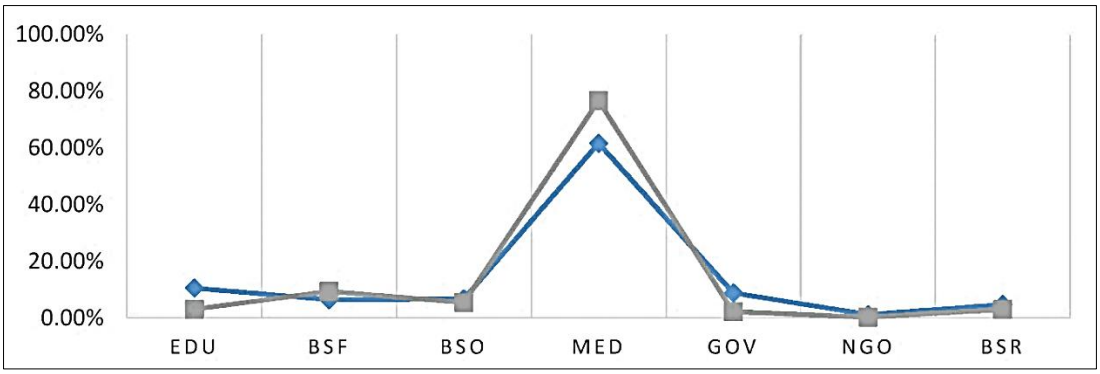


**Figure 5.** Healthcare cloud security breaches

The hybrid cloud architecture allows for the integration of several deployment types yet maintains appropriate balances and allows information and service mobility. Although risks in hybrid clouds are addressed, attacks remain potential at collocation points among various cloud models. Figure 4 exhibits the effectiveness of cloud storage providers. Figure 5 represents the percentage of healthcare cloud security vulnerabilities.

### *2. Security in the Service Delivery Model*

Cloud service companies primarily offer three delivery methods: SaaS, PaaS, and IaaS, often known as provisioning and delivery methods. The IaaS layer delivers the basic cloud infrastructure on a subscription basis to

consumers. Infrastructure refers to the fundamental physical elements and the software that manages them, which comprises computers, networking, memory, system files, and software platforms. The virtual environment and the physical environment are the two most important factors for safeguarding the IaaS layer. At the virtual level, certain security needs must be met, including network access, encryption techniques, implementation of security routes, and online security. In terms of physical elements, it is necessary to assure hardware dependability while also avoiding physical infiltration.

PaaS is the application deployment level, wherein programmers are expected to build and execute their programs. Some studies, however, regard PaaS and IaaS to be part of the same layer instead of separate. A platform often permits the use of technology platforms, analytics, and services. Nevertheless, software providers currently support a restricted set of programming tools and APIs. PaaS security needs are nearly identical to that of IaaS, and both contain virtual environment features. If there are discrepancies in security procedures, they are connected to the system level or the role of the service user, such as a programmer or system administrator. Users (tenants) such as employees, supervisors, customers, and inspectors often use SaaS over the network.

## 5. CLOUD SECURITY CONTROLS

Cloud security controls are a collection of measures that allow cloud infrastructure to guard against vulnerabilities and minimize or decrease the impact of a cyberattacks. It is a comprehensive concept that encompasses everything from policies, processes, and rules to be established in order to safeguard a cloud-based computing system. Although there are several kinds of control underlying cloud security infrastructure, these often fall within one of the main groups as given below.

### *A. Deterrent controls*

These restrictions are designed to limit distributed cloud threats. They do not defend the cloud platform or services, but rather act as a notification to a possible attacker.

### *B. Preventive controls*

These controls are employed to manage, reinforce, and safeguard a cloud's vulnerabilities. A robust cloud authentication process, for example, reduces the likelihood that unauthorized individuals would get into cloud-based services but more probable that cloud customers will be properly recognized.

### *C. Detective controls*

Detective control is an accountancy terminology for a variety of internal control used to identify flaws in a secured network. Detective control could be used to achieve a variety of objectives, including quality assurance, credit monitoring, and compliance requirements.

### *D. Corrective controls*

These controls are intended to fix problems or dangers and avoid them from happening again. They start whenever negative results are recognized and maintain the light on the issue unless the administration is able to fix the problem as well as rectify the issue.

## 6. DATA SECURITY AND PRIVACY

Cloud computing information security entails not only encryption technology. Information security needs differ depending on the three different service models: SaaS, PaaS, and IaaS. Data at Rest refers to information kept in the cloud, and Data in Transit refers to data traveling between and within the cloud, these are the two states of information that generally pose a danger to its safety in clouds. The type of information security measures, techniques, and procedures determine integrity and confidentiality. Table 2 displays the information security advancements made possible by cloud algorithms.

**Table 2.** Data security enhancements using cloud algorithms

| Algorithm | Performance | Advantages | Disadvantages |
|---|---|---|---|
| **C-RANS** | Uses stochastic geometry-based network model, thereby attaining efficient capacity | Effective capacity, and energy efficiency | Performance can be further enhanced by integrating RRU & RRH allocations |
| **Data Vaporizer** | Secret sharing of keys to improve security and reliability | Storage cost is minimum | Design of configurable data storage framework above the low-cost cloud storage |
| **Public integrity auditing scheme** | A cloud server will collude with revoked users for deceiving TPAs that stored files are kept safe even if the complete file was deleted | Attains secured auditing scheme efficiency | Above attacks |
| **ID-PUIC** | Checks data integrity of public and private cloud security | Improves the cloud performance | Increase computational overheads |

### *1. Data integrity*

Data integrity is considered one of the most important aspects of every data system. In essence, data integrity refers to the protection of information against unlawful destruction, alteration, or falsification. Controlling an individual's access and permissions to certain organizational assets guarantees that critical information and applications are not misused, exploited, or destroyed. Data integrity is readily established in a standalone system with a single database.

Data integrity in an independent system is protected by network restrictions and operations, that is typically completed by a database management system (DBMS). To maintain data integrity, operations must adhere to ACID (Atomicity, Consistency, Isolation, and Durability) criteria. Many databases implement ACID transactions and can

maintain data integrity. Information access is managed via authentication. It is the technique that a network decides what type of access an authenticated person must have in order to safeguard the platform's capabilities.

Data integrity in a cloud environment involves ensuring reliability. Unauthorized individuals must not lose or change information. Data integrity is the foundation for providing cloud computing solutions including SaaS, PaaS, and IaaS.

***2. Data confidentiality***

Data confidentiality is essential for customers storing sensitive or confidential information in the cloud. To maintain data confidentiality, authentication and control over access mechanisms are employed. Data confidentiality, identification, and security systems challenges in cloud technology might be solved by strengthening cloud dependability and dependability.

Although customers need not regard cloud services and it is nearly difficult for cloud-based storage service companies to eradicate possible intrusion attempts, it is extremely unsafe for individuals to store critical information directly in cloud services. One of the most important issues is the vulnerability of information in the previously indicated states.

***a. Data at Rest***

Data at rest relates to the information stored in the cloud or any information that may be accessed using the Internet. This covers both data backups and active information. As previously stated, enterprises that fail to manage a cloud service may find it challenging to safeguard data at rest because they do not have direct control over the information. This problem, nevertheless, may be remedied by keeping a private cloud with tightly regulated accessibility.

***b. Data in Transit***

Data in transit often entails information that is going into and leaving the cloud. This information could take the format of a document or database saved on the cloud and retrieved for usage in another place. Whenever information is transferred to the cloud, it is referred to as data in transit. Data in transit, such as login credentials and passwords, may sometimes be secured. Nonetheless, data in unstructured format is also data in transit.

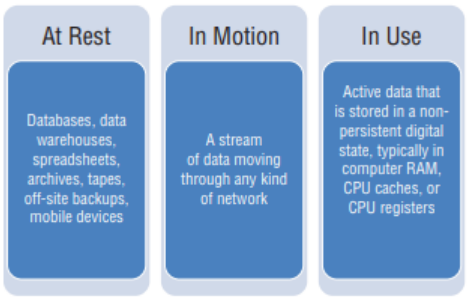


**Figure 6.** Data States at Rest and in Transit

Data in transit is frequently more vulnerable to danger than data at rest since this should transfer from one location to another (Figure 6). Intermediating software may spy on the information and occasionally modify it on its journey

to the target in a number of ways. Cryptography provides one of the most effective ways of protecting data in transit.

## 7. SAFEGUARDING CLOUD DATA BY ENCRYPTION

Various cryptographic algorithms may be used for data at rest and data in transit. Cryptographic keys for data in transit, for instance, might be brief, but credentials for data at rest could be held for extended periods.

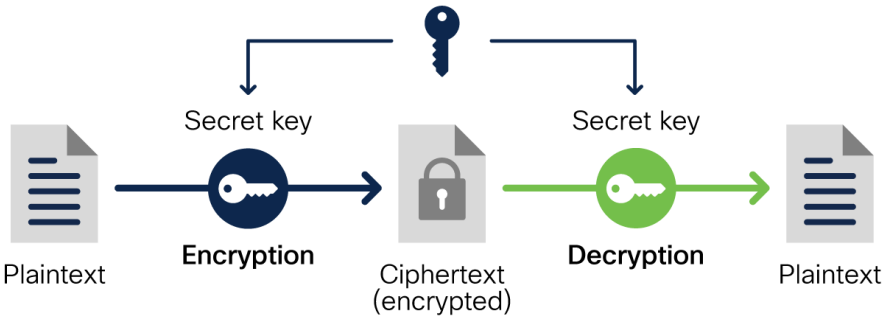


**Figure 7.** Process of Fundamental Cryptography

Nowadays, several cryptography algorithms are employed to encrypt information. Cryptography provides stronger information security compared to ever before for assured information security, authenticity, and reliability. The message is converted into cipher text using an encryption method, and the resultant cipher text is decoded using a decryption key, as demonstrated in Figure 7. Encryption technology has three primary applications:

### A. In the case of Block Ciphers

A block cipher is a technique for securing information (creating cipher text) that applies an encryption algorithm and method to a block of data rather than one bit at a period. This approach ensures that comparable sections of text in a text are not encoded in a similar manner. The cipher text from the previously encoded block is generally applied to the following block in a sequence. As seen in Figure 8, plain text is broken into information blocks of 64 bits in size. These blocks are subsequently encoded with an encryption key to produce cipher text.

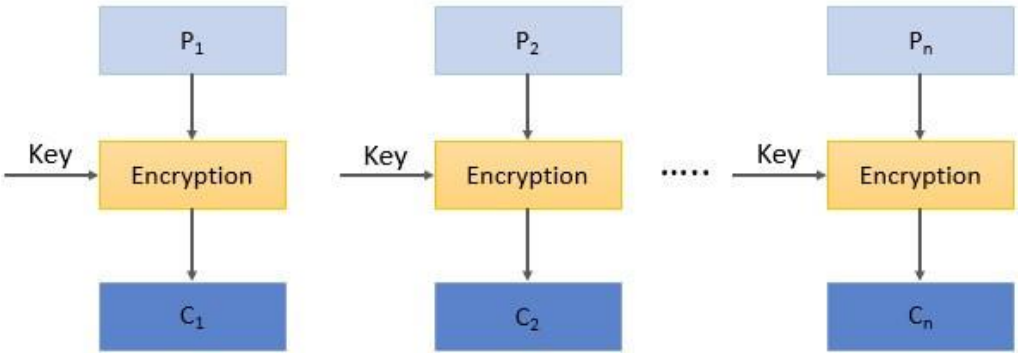


**Figure 8.** Block Cipher Encryption Mechanism

### B. As Stream Ciphers

This method of securing information is also known as a state cipher because it is dependent on the current state of the cipher. Instead of blocks of data, each bit is encoded in this technology. Each bit is subjected to an encryption

key and a technique one at a time. Because of their low hardware expense, encryption algorithms are often quicker to provide than block ciphers. However, if not utilized correctly, this strategy may lead to serious security issues.

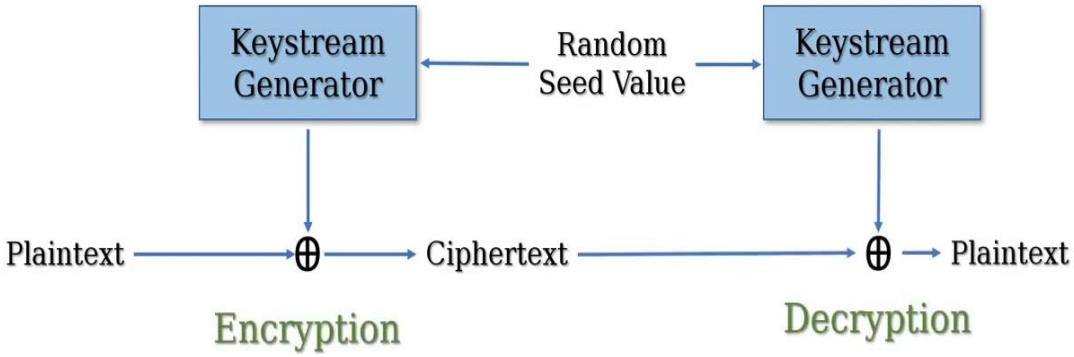


**Figure 9.** Operation of Stream Cipher Encryption/Decryption

Stream cipher, as seen in Figure 9, encrypt an individual bit rather than a block of text using an encryption key. The cipher text produced is a sequence of encrypted bits that may be quickly decoded utilizing a decryption key to generate fresh plain text.

### C. In the Case of Hash Functions

A mathematical formula known as a hash function is utilized in this approach to convert text information into an alphabetic string. Typically, the length of the generated alphabetic string is fixed. This method ensures that no two strings may contain the same alphabetic string as a result. Even if the input strings are marginally diverse, there is a chance of significant disparity between the result strings created by them. This hash function may be a very basic mathematical function, as seen in Figure 10.

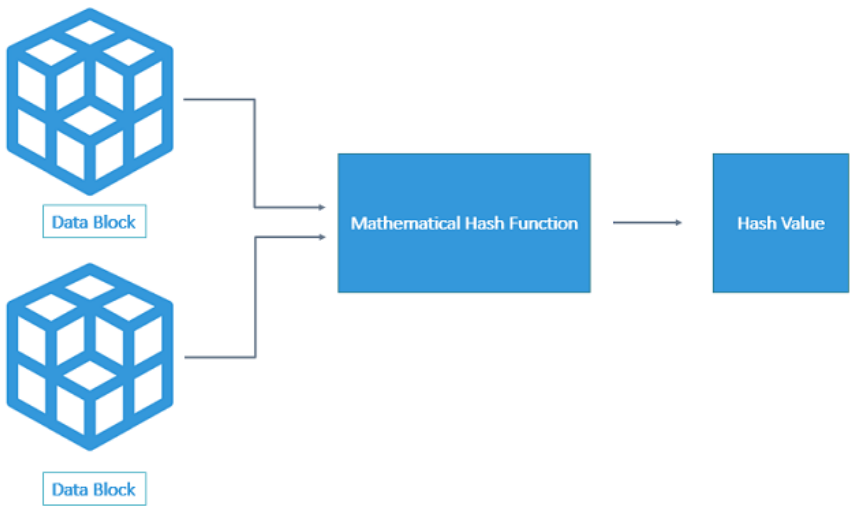


**Figure 10.** Principle of Cryptographic Hash Functions

Many of these, in addition to the previously described techniques and approaches, are widely utilized in protecting data in the cloud to protect the information. The application of these approaches differs depending on the situation. Whatever approach is employed, it is strongly advised to maintain information security in both private and public clouds. Table 3 provides an examination of contemporary cloud services.

**Table 3.** Comparison of different cloud services

| Cloud service | Protection against brute-force attacks | Two-factor authentication | Pass recovery mechanism | SCC formation protocol | Message authentication procedure | Key agreement procedure | Data encryption procedure |
|---|---|---|---|---|---|---|---|
| **DropBox** | Temporary lock | OTP & Passwords | Present | TLS 1.1 | SHA1 | ECDHE_RSA | AES-256 |
| **Google Drive** | Using characters from images | OTP & Passwords | Present | TLS 1.1 | SHA1 | ECDHE_ECDSA | - |
| **Wuala** | Absent | Absent | Absent | Absent | SHA1 | DHE_RSA | Converged encryption method |

## 8. CONCLUSION

The primary objective of this paper is to investigate and assess information security approaches in cloud applications. Also, examination and assessment are done over the most critical data security measures that have already been approved by cloud computing service providers. The methods are summarised into four categories based on the security measures they offer like authentication, encryption, security systems, and authorization. Moreover, focus is done on the cybersecurity threats that must be addressed thoroughly in order to ensure good data protection in the cloud. Discussions are made in terms of critical security steps for cloud information security that need to be implemented. Suggestions over a number of problems are mentioned to examine in order to strengthen information security, such as correct use of administrative rights, wireless connectivity control of information in systems that employ wireless communications, backup and recovery, and cloud border defense.

## REFERENCES

[1] A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, “Data security in cloud computing”, in 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), 2016, pp. 55–59.

[2] A. S. Ibrahim, J. Hamlyn-Harris, and J. Grundy, “Emerging security challenges of cloud virtual infrastructure”, arXiv Prepr. arXiv1612.09059, 2016.

[3] C. I. Fan and S. Y. Huang, “Controllable privacy preserving search based on symmetric predicate encryption in cloud storage”, Future Generation Computer Systems, 29(7), (2013), 1716-1724.

[4] C. McCarthy, K. Sullivan, and R. Krishnan, “Systems and methods for private cloud computing.” Google Patents, 23-Jul-2013.

[5] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, “Secure integration of IoT and cloud computing”, Futur. Gener. Comput. Syst., vol. 78, pp. 964–975, 2018.

[6] B. Samanthula, Y. Elmehdwi, G. Howser and S. Madria, "A secure data sharing and query processing framework via federation of cloud computing", Information Systems, vol. 48, pp. 196-212, 2015.

[7] D. W. Chadwick and K. Fatema, "A privacy preserving authorization system for the cloud", Journal of Computer and System Sciences, 78(5), (2012), 1359-1373.

[8] F. Farokhi, I. Shames, and N. Batterham, "Secure and private cloud-based control using semi-homomorphic encryption", IFAC-PapersOnLine, vol. 49, No. 22, pp. 163–168, 2016.

[9] Anil Lamba, "A role of data mining analysis to identify suspicious activity alert system", International Journal for Technological Research in Engineering, Vol. 2 Iss. 3, pp. 5814–5825, 2014.

[10] G. Ramachandra, M. Iftikhar, and F. A. Khan, "A comprehensive survey on security in cloud computing", Procedia Comput. Sci., vol. 110, pp. 465–472, 2017.

[11] G. Wang, Q. Liu, J. Wu and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Computers & Security, 30(5), (2011), 320-331.

[12] Anil Lamba, "A study paper on security related issue before adopting cloud computing service model", International Journal for Technological Research in Engineering, Vol. 3 Iss. 4, pp. 5837–5840, 2015.

[13] K. Selvakumar and M. Prabakaran, "An Analysis for Security Issues and their Solutions in Cloud Computing", 2018.

[14] L. Badger, T. Grance, R. Patt-Corner and J. Voas, "Cloud computing synopsis and recommendations (draft), nist special publication 800-146", Recommendations of the National Institute of Standards and Technology, Tech. Rep. (2011).

[15] M. Hange, "Security Recommendations for Cloud Computing Providers", Federal Office for Information Security (2011).

[16] M. Nieles, K. Dempsey, and V. Pillitteri, "An introduction to information security", National Institute of Standards and Technology, 2017.

[17] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues", J. Netw. Comput. Appl., vol. 43, pp. 121–141, 2014.

[18] Anil Lamba, "S4: A novel & secure method for enforcing privacy in cloud data warehouses", International Journal for Technological Research in Engineering, Vol. 3, Iss. 8, pp. 5707–5710, 2016.

[19] N. Surv, B. Wanve, R. Kamble, S. Patil, and J. Katti, "Framework for client side AES encryption technique in cloud computing", in 2015 IEEE International Advance Computing Conference (IACC), 2015, pp. 525–528.

[20] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring data security issues and solutions in cloud computing", Procedia Comput. Sci., vol. 125, pp. 691–697, 2018.

[21] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring security issues and solutions in cloud computing services-a survey", Cybern. Inf. Technol., vol. 17, No. 4, pp. 3–31, 2017.

[22] Anil Lamba, "A comprehensive survey on security in cloud computing", International Journal for Technological Research in Engineering, International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS - 2016), pp. 31-34, 2017.

[23] S. Aldossary and W. Allen, "Data security, privacy, availability and integrity in cloud computing: issues and current solutions", Int. J. Adv. Comput. Sci. Appl., vol. 7, No. 4, pp. 485–498, 2016.

[24] S. Goyal, "Public vs private vs hybrid vs community-cloud computing: a critical review", Int. J. Comput. Netw. Inf. Secur., vol. 6, No. 3, p. 20, 2014.

[25] S. H. H. Madni, M. S. A. Latiff, and Y. Coulibaly, "Resource scheduling for infrastructure as a service (IaaS) in cloud computing: Challenges and opportunities", J. Netw. Comput. Appl., vol. 68, pp. 173–200, 2016.

[26] Sunumol Cherian, Kavitha Murukezhan, "Providing Data Protection as a Service in Cloud Computing" International Journal of Scientific and Research Publications, Volume 3, Issue 6, (2013) 1 ISSN 2250-3153.

[27] T. Acar, M. Belenkiy and A. Küpçü, "Single password authentication", Computer Networks, 57(13), (2013), 2597-2614.

[28] T. Islam, D. Manivannan, and S. Zeadally, "A classification and characterization of security threats in cloud computing", Int. J. Next-Gener. Comput, vol. 7, No. 1, 2016.

[29] Anil Lamba, "Uses of cluster computing techniques to perform big data analytics for smart grid automation system", International Journal for Technological Research in Engineering, Vol. 1, Iss. 7, pp. 5804-5808, 2014.

[30] V. R. Pancholi and B. P. Patel, "Enhancement of cloud computing security with secure data storage using AES", Int. J. Innov. Res. Sci. Technol., vol. 2, No. 9, pp. 18–21, 2016.

[31] Varsha, Amit Wadhwa, Swati Gupta, "Study of Security Issues in Cloud Computing" IJCSMC, Vol. 4, Issue. 6, (2015), pg.230 – 234, ISSN 2320–088X

[32] W. Van Geit et al=., "BluePyOpt: leveraging open source software and cloud infrastructure to optimise model parameters in neuroscience", Front. Neuroinform., vol. 10, p. 17, 2016.

[33] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability", in 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2017, pp. 468–477.